Family list
1 family member for:
JP2002269043
Derived from 1 application.

1 **INFORMATION PROCESSOR, INFORMATION PROCESSING SYSTEM, USER AUTHENTICATION PROCESSING METHOD AND STORAGE MEDIUM**
Publication info: **JP2002269043 A** - 2002-09-20

Data supplied from the ***esp@cenet*** database - Worldwide

THIS PAGE BLANK (USPTO)

INFORMATION PROCESSOR, INFORMATION PROCESSING SYSTEM, USER AUTHENTICATION PROCESSING METHOD AND STORAGE MEDIUM

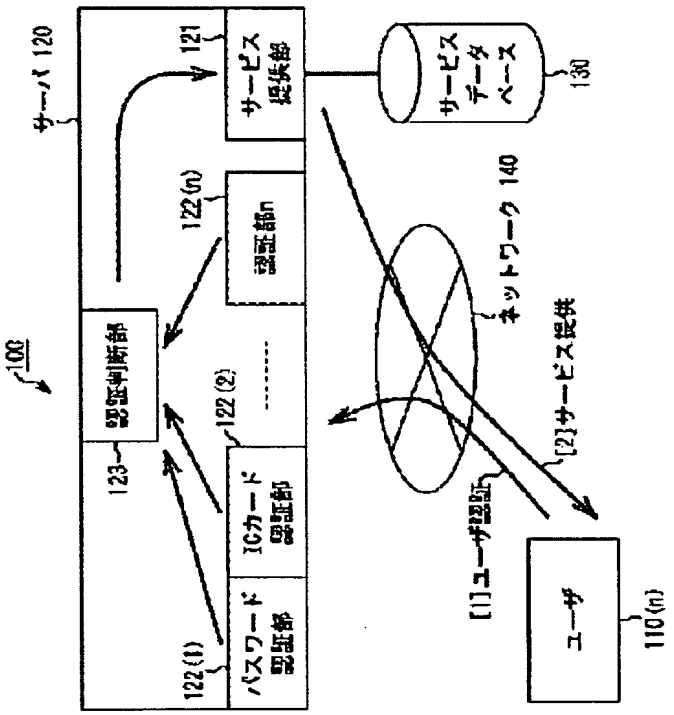
Patent number: JP2002269043
Publication date: 2002-09-20

Inventor: TAGASHIRA NOBUHIRO; SUGA YUJI; WAKAO SATOSHI
Applicant: CANON KK

Classification:
- international: G06F15/00; H04L9/32
- european:
Application number: JP20010067211 20010309
Priority number(s): JP20010067211 20010309

Abstract of **JP2002269043**

PROBLEM TO BE SOLVED: To provide an information processing system corresponding to various service supply forms. SOLUTION: In an information processor 120 authenticating a user based on information by a request from a user 110(n), user authentication means 122 (1), 1220(2),..., and 122(n) authenticate the user by an arbitrary user authentication method. An authentication judging means 123 finally decides a stepwise user authentication result with respect to the user based on the authentication results in the user authentication means 122(1), 1220(2),..., and 122(n).



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－269043
（P2002－269043A）
(43)公開日　平成14年９月20日(2002.9.20)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｃ０６Ｆ　15/00	３３０Ｄ	５Ｂ０８５
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	５Ｊ１０４
			６７３Ｄ	
			６７３Ｅ	
			６７５Ｄ	

審査請求　未請求　請求項の数15　ＯＬ　（全 17 頁）

(21)出願番号　特願2001－67211(P2001－67211)

(22)出願日　平成13年３月９日(2001.3.9)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　田頭　信博
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

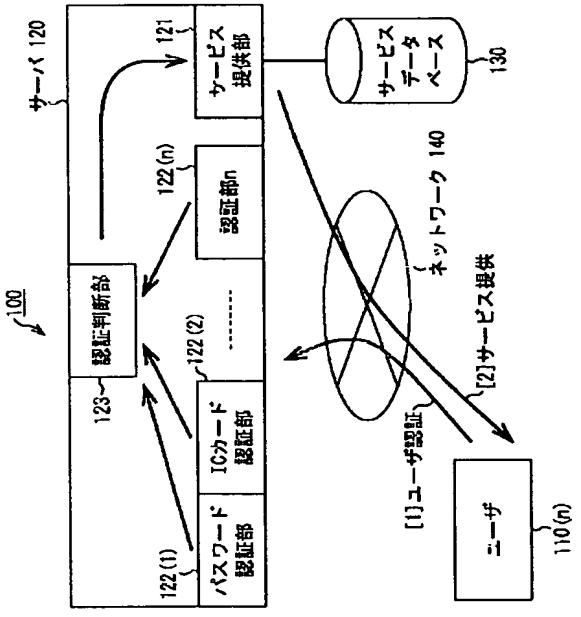
(72)発明者　須賀　祐治
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

(74)代理人　100090273
弁理士　國分　孝悦

最終頁に続く

(54)【発明の名称】　情報処理装置、情報処理システム、ユーザ認証処理方法、及び記憶媒体

(57)【要約】
【課題】　多様なサービス提供形態に対応できる情報処理システムを提供する。
【解決手段】　ユーザ１１０（ｎ）からの要求による情報に基づいて、当該ユーザ認証を行う情報処理装置１２０において、ユーザ認証手段１２２（１），１２２０（２），…，１２２（ｎ）は、任意のユーザ認証方法によりユーザ認証を行う。認証判断手段１２３は、ユーザ認証手段１２２（１），１２２０（２），…，１２２（ｎ）での認証結果に基づいて、ユーザに対する段階的なユーザ認証結果を最終決定する。



【特許請求の範囲】
【請求項１】　ユーザからの要求による情報に基づいて、当該ユーザ認証を行う情報処理装置であって、
任意のユーザ認証方法により上記ユーザ認証を行う少なくとも１つのユーザ認証手段と、
上記ユーザ認証手段での認証結果に基づいて、上記ユーザに対する段階的なユーザ認証結果を決定する認証判断手段とを備えることを特徴とする情報処理装置。
【請求項２】　上記認証判断手段は、複数の上記ユーザ認証手段での複数の認証結果の組み合わせに基づいて、上記ユーザに対する段階的なユーザ認証結果を決定することを特徴とする請求項１記載の情報処理装置。
【請求項３】　ユーザからの要求による情報に基づいて、当該ユーザ認証を行う情報処理装置であって、
任意のユーザ認証方法により上記ユーザ認証を行う少なくとも１つのユーザ認証手段と、
上記ユーザの存在位置を検出する検出手段と、
上記ユーザ認証手段での認証結果及び上記検出手段での検出結果に基づいて、上記ユーザに対する段階的なユーザ認証結果を決定する認証判断手段とを備えることを特徴とする情報処理装置。
【請求項４】　上記認証判断手段は、複数の上記ユーザ認証手段での複数の認証結果の組み合わせ、及び上記検出手段での検出結果に基づいて、上記ユーザに対する段階的なユーザ認証結果を決定することを特徴とする請求項３記載の情報処理装置。
【請求項５】　上記ユーザ認証方法は、パスワードを用いた認証方法、情報記録された記憶媒体を用いた認証方法、及びバイオメトリクスを用いた認証方法の少なくとも何れかの方法を含むことを特徴とする請求項１又は３記載の情報処理装置。
【請求項６】　上記認証判断手段で決定されたユーザ認証結果に基づいて、上記ユーザに対して任意のサービスを提供するサービス提供手段を備えることを特徴とする請求項１又は３記載の情報処理装置。
【請求項７】　上記サービス提供手段は、段階的な上記サービスを提供することを特徴とする請求項６記載の情報処理装置。
【請求項８】　複数の機器が互いに通信可能に接続されてなる情報処理システムであって、
上記複数の機器のうち少なくとも１つの機器は、請求項１～７の何れかに記載の情報処理装置の機能を有することを特徴とする情報処理システム。
【請求項９】　ユーザからの要求に基づいて、当該ユーザ認証を行うためのユーザ認証処理方法であって、
上記ユーザに対してユーザ認証を行う単一又は複数のユーザ認証ステップと、
上記単一又は複数のユーザ認証ステップによる認証結果の組み合わせに基づいて、段階的なユーザ認証結果を最終決定する認証判断ステップとを含むことを特徴とするユーザ認証処理方法。
【請求項１０】　ユーザからの要求に基づいて、当該ユーザ認証を行うためのユーザ認証処理方法であって、
上記ユーザに対してユーザ認証を行う単一又は複数のユーザ認証ステップと、
上記ユーザからの要求がなされた装置或いはシステムの位置情報を検出する位置検出ステップと、
上記単一又は複数のユーザ認証ステップによる認証結果の組み合わせ、及び上記位置検出ステップによる検出結果に基づいて、段階的なユーザ認証結果を最終決定する認証判断ステップとを含むことを特徴とするユーザ認証処理方法。
【請求項１１】　上記単一又は複数のユーザ認証ステップは、パスワードを用いたユーザ認証を行うステップ、情報記録された記憶媒体を用いたユーザ認証を行うステップ、及びバイオメトリクスを用いたユーザ認証を行うステップの少なくとも何れかのステップを含むことを特徴とする請求項９又は１０記載のユーザ認証処理方法。
【請求項１２】　上記認証判断ステップにより最終決定されたユーザ認証結果に基づいて、上記ユーザ側に対して任意のサービスを提供するサービス提供ステップを含むことを特徴とする請求項９又は１０記載のユーザ認証処理方法。
【請求項１３】　上記サービス提供ステップは、段階的な上記サービスを提供するステップを含むことを特徴とする請求項１２記載のユーザ認証処理方法。
【請求項１４】　請求項１～７の何れかに記載の情報処理装置の機能、又は請求項８記載の情報処理システムの機能をコンピュータに実現させるためのプログラムを記録したコンピュータ読出可能な記憶媒体。
【請求項１５】　請求項９～１３の何れかに記載のユーザ認証処理方法の処理ステップをコンピュータに実行させるためのプログラムを記録したコンピュータ読取可能な記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えば、ネットワークを介したサービス享受のためのユーザ認証を行う装置或いはシステムに用いられる、情報処理装置、情報処理システム、ユーザ認証処理方法、及びそれを実施するための処理ステップをコンピュータが読出可能に格納した記憶媒体に関するものである。
【０００２】
【従来の技術】近年において、インターネットに代表されるネットワークインフラの普及に伴い、ネットワークを利用したサービスが多く提供されるようになった。これらのサービスの中では、“ａｎｏｎｙｍｏｕｓ　ｆｔｐ”に代表されるような、ユーザ認証（ユーザ名とパスワード等を用いた認証）を伴わないサービスが存在するが、“Ｔｅｌｎｅｔ（ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉ

on network)"及び"rlogin(remote login)"等のような、ユーザ認証を伴うサービスが多く存在する。このような背景のもと、ユーザ認証の方法としては、パスワードやICカード、或いはバイオメトリクス等を用いた様々な方法が提案され実現されている。

【0003】具体的には例えば、ユーザ認証の方法としては、銀行のCDやATMの利用時のパスワード入力による方法、或いは"Telnet"や"rlogin"等のサービスを受ける際のパスワード入力による方法がある。また、建物への入退出管理や計算機利用の管理等を行なうためのICカードによるユーザ認証方法や、高度な機密保持が必要な建物への入退出管理を行うための指紋や網膜等によるユーザ認証(バイオメトリクス技術を用いたユーザ認証)方法がある。

【0004】また、近年のLAN網や、固定電話回線網、或いは無線電話回線網等のネットワークインフラの多様化によって、ユーザがサービスを享受するための端末装置の多様化も進んでいる。

【0005】上記の端末装置としては、例えば、パーソナルコンピュータ(以下、単に「パソコン」又は「PC」と言う)が多く利用されている。一般にパソコンはユーザの自宅で利用されるが、近年では、パソコンを店内に設けた所謂インターネットカフェが多く利用されている。これにより、ユーザは、自宅のPCでサービスを享受することが可能であると共に、インターネットカフェのPCでサービスを享受することも可能である。

【0006】さらに、上記の端末装置としては、ネットワークを介した通信が可能な携帯電話等の携帯端末装置が利用されており、この携帯端末装置を利用したサービス享受や、上述したPC等を利用したサービス享受等、様々なサービス利用形態が存在している。

【0007】

【発明が解決しようとする課題】しかしながら、上述したような従来のユーザ認証方法は、ユーザに提供するサービスに対して固定の方法のみしか存在しない。例えば、"Telnet"や"rlogin"によるサービス享受のためのユーザ認証は、簡便なパスワードによる方法が用いられている。また、高度に機密保持が必要な建物への入退出管理のためのユーザ認証は、高度なユーザ認証技術であるバイオメトリクスによる方法が用いられている。

【0008】すなわち、従来のユーザ認証方法は、簡便な認証であるか、或いは厳密な認証であるかの差はあるが、何れの認証においても、その認証結果は、「可」又は「不可」の二通りしかない。このため、ユーザ認証結果に応じて、例えば、「サービスを提供する」又は「サービスを提供しない」の二通りの判断しか行えない。したがって、以下に説明するような問題が生じてくる。

【0009】例えば、今後は、ユーザが使用する端末装置の多様化により、段階的なサービスの提供が考えられる。具体的には、画像を閲覧するサービスに関して、高解像度の画像を表示可能な自宅のPCにおいてサービスを享受する場合と、低解像度の画像(場合によっては二値画像)しか表示できない携帯端末装置からサービスを享受する場合とでは、同じサービスであっても、そのサービスの品質にレベル差がある。また、機密文書を閲覧するサービスに関して、社内から社内の機密文書にアクセスする等の地理的に安全な場所に位置する端末装置からサービスを享受する場合と、社外から社内の機密文書にアクセスする等の地理的に安全でない場所に位置する端末装置からサービスを享受する場合とでは、同じサービスであっても、そのサービスの機密度合いにレベル差がある。

【0010】しかしながら、上述したように、従来のユーザ認証方法は、提供するサービスに固有のものであり、その認証結果が「可」又は「不可」の二通りしかない、すなわち「サービスを提供する」又は「サービスを提供しない」の二通りの判断しか行えないため、上記のような段階的なサービス提供等の様々なサービス提供形態に適応的に対応できない。

【0011】そこで、本発明は、上記の欠点を除去するために成されたもので、以下の(1)～(3)を実現可能な、情報処理装置、情報処理システム、ユーザ認証処理方法、及びそれを実施するための処理ステップをコンピュータが読出可能に格納した記憶媒体を提供することを目的とする。

(1)多様なサービス提供形態に対応できる。

(2)段階的であって多様なサービスを提供する際に、それぞれのサービスに対応可能である。

(3)ユーザ認証結果に応じて適応的に異なるサービスを提供できる。

【0012】

【課題を解決するための手段】斯かる目的下において、第1の発明は、ユーザからの要求による情報に基づいて、当該ユーザ認証を行う情報処理装置であって、任意のユーザ認証方法により上記ユーザ認証を行う少なくとも1つのユーザ認証手段と、上記ユーザ認証手段での認証結果に基づいて、上記ユーザに対する段階的なユーザ認証結果を決定する認証判断手段とを備えることを特徴とする。

【0013】第2の発明は、上記第1の発明において、上記認証判断手段は、複数の上記ユーザ認証手段での複数の認証結果の組み合わせに基づいて、上記ユーザに対する段階的なユーザ認証結果を決定することを特徴とする。

【0014】第3の発明は、ユーザからの要求による情報に基づいて、当該ユーザ認証を行う情報処理装置であって、任意のユーザ認証方法により上記ユーザ認証を行う少なくとも1つのユーザ認証手段と、上記ユーザの存

在位置を検出する検出手段と、上記ユーザ認証手段での認証結果及び上記検出手段での検出結果に基づいて、上記ユーザに対する段階的なユーザ認証結果を決定する認証判断手段とを備えることを特徴とする。

【００１５】第４の発明は、上記第３の発明において、上記認証判断手段は、複数の上記ユーザ認証手段での複数の認証結果の組み合わせ、及び上記検出手段での検出結果に基づいて、上記ユーザに対する段階的なユーザ認証結果を決定することを特徴とする。

【００１６】第５の発明は、上記第１又は３の発明において、上記ユーザ認証方法は、パスワードを用いた認証方法、情報記録された記憶媒体を用いた認証方法、及びバイオメトリクスを用いた認証方法の少なくとも何れかの方法を含むことを特徴とする。

【００１７】第６の発明は、上記第１又は３の発明において、上記認証判断手段で決定されたユーザ認証結果に基づいて、上記ユーザに対して任意のサービスを提供するサービス提供手段を備えることを特徴とする。

【００１８】第７の発明は、上記第６の発明において、上記サービス提供手段は、段階的な上記サービスを提供することを特徴とする。

【００１９】第８の発明は、複数の機器が互いに通信可能に接続されてなる情報処理システムであって、上記複数の機器のうち少なくとも１つの機器は、請求項１～７の何れかに記載の情報処理装置の機能を有することを特徴とする。

【００２０】第９の発明は、ユーザからの要求に基づいて、当該ユーザ認証を行うためのユーザ認証処理方法であって、上記ユーザに対してユーザ認証を行う単一又は複数のユーザ認証ステップと、上記単一又は複数のユーザ認証ステップによる認証結果の組み合わせに基づいて、段階的なユーザ認証結果を最終決定する認証判断ステップとを含むことを特徴とする。

【００２１】第１０の発明は、ユーザからの要求に基づいて、当該ユーザ認証を行うためのユーザ認証処理方法であって、上記ユーザに対してユーザ認証を行う単一又は複数のユーザ認証ステップと、上記ユーザからの要求がなされた装置或いはシステムの位置情報を検出する位置検出ステップと、上記単一又は複数のユーザ認証ステップによる認証結果の組み合わせ、及び上記位置検出ステップによる検出結果に基づいて、段階的なユーザ認証結果を最終決定する認証判断ステップとを含むことを特徴とする。

【００２２】第１１の発明は、上記第９又は１０の発明において、上記単一又は複数のユーザ認証ステップは、パスワードを用いたユーザ認証を行うステップ、情報記録された記憶媒体を用いたユーザ認証を行うステップ、及びバイオメトリクスを用いたユーザ認証を行うステップの少なくとも何れかのステップを含むことを特徴とする。

【００２３】第１２の発明は、上記第９又は１０の発明において、上記認証判断ステップにより最終決定されたユーザ認証結果に基づいて、上記ユーザ側に対して任意のサービスを提供するサービス提供ステップを含むことを特徴とする。

【００２４】第１３の発明は、上記第１２の発明において、上記サービス提供ステップは、段階的な上記サービスを提供するステップを含むことを特徴とする。

【００２５】第１４の発明は、請求項１～７の何れかに記載の情報処理装置の機能、又は請求項８記載の情報処理システムの機能をコンピュータに実現させるためのプログラムをコンピュータ読出可能な記憶媒体に記録したことを特徴とする。

【００２６】第１５の発明は、請求項９～１３の何れかに記載のユーザ認証処理方法の処理ステップをコンピュータに実行させるためのプログラムをコンピュータ読出可能な記憶媒体に記録したことを特徴とする。

【００２７】

【発明の実施の形態】以下、本発明の実施の形態について図面を用いて説明する。

【００２８】〔第１の実施の形態〕本発明は、例えば、図１に示すようなネットワークシステム１００に適用される。

【００２９】まず、本実施の形態のネットワークシステム１００の具体的な説明の前に、本実施の形態での基本とする目的は、多様なサービスを提供するために多様なユーザ認証結果を得ることである。本実施の形態における“多様なユーザ認証結果”とは、従来のようなユーザ認証結果としての「可」又は「不可」の二値の結果ではなく、多値の結果を意味する。

【００３０】多値のユーザ認証結果を得るための構成としては様々なものが考えられる。例えば、パスワードを用いたユーザ認証では、入力されたパスワードの文字数に対する合致した文字数の割合に基づいて、ユーザ認証結果を多値で出力する。また、指紋を用いたユーザ認証では、指紋画像の類似度合いに基づいて、ユーザ認証結果を多値で出力する。

【００３１】しかしながら、あるユーザ認証方法においてユーザ認証結果を多値化した場合でも、最終的なユーザ認証結果の決定に作用する情報は１種類のみである。例えば、パスワードを用いたユーザ認証では、当該パスワードの文字列情報のみが、ユーザ認証結果の決定に作用する。また、指紋を用いたユーザ認証では、指紋画像のみが、ユーザ認証結果の決定に作用する。

【００３２】すなわち、多様なサービスを提供するための多様なユーザ認証結果を得る構成としては、ユーザ認証方法に依存した１種類の情報からの多値のユーザ認証結果だけでは、十分な多様性を持つことができないと考えられる。

【００３３】そこで、本実施の形態のネットワークシス

テム１００では、以下に説明するような構成により、独立した複数のユーザ認証方法（以下、「ユーザ認証方式」とも言う）により多様なユーザ認証結果を得ることを実現している。

【００３４】＜ネットワークシステム１００の全体構成＞ネットワークシステム１００は、上記図１に示すように、ユーザ側の端末装置１１０（ｎ）と、サービスデータベース１３０を有するサーバ１２０（ｍ）とが、ネットワーク１４０を介して互いに通信可能なように接続された構成としている。

【００３５】尚、上記図１では、説明の簡単のため、ネットワーク１４０に接続されているユーザ側の端末装置として、１つのユーザ側の端末装置１１０（ｎ）のみ図示しているが、この接続数に限られることはない。本実施の形態では、例えば、複数のユーザ側の端末装置がネットワーク１４０に接続されており、これらの複数のユーザ側の端末装置の中の任意の端末装置１１０（ｎ）に着目している。また、サーバ１２０についても同様に、ネットワーク１４０に接続されているサーバとして、１つのサーバ１２０のみ図示しているが、この接続数に限られることはない。

【００３６】ユーザ側の端末装置１１０（ｎ）、及びサーバ１２０は、例えば、図２に示すようなコンピュータ機能２００により、後述するような各種機能を実現するようになされている。

【００３７】コンピュータ機能２００は、上記図２に示すように、ＣＰＵ２０１と、ＲＯＭ２０２と、ＲＡＭ２０３と、キーボード（ＫＢ）２０９のキーボードコントローラ（ＫＢＣ）２０５と、表示部としてのＣＲＴディスプレイ（ＣＲＴ）２１０のＣＲＴコントローラ（ＣＲＴＣ）２０６と、ハードディスク（ＨＤ）２１１及びフロッピー（登録商標）ディスク（ＦＤ）２１２のディスクコントローラ（ＤＫＣ）２０７と、ネットワーク１４０に接続されたネットワークインターフェースカード（ＮＩＣ）２０８とが、システムバス２０４を介して互いに通信可能に接続された構成としている。

【００３８】ＣＰＵ２０１は、ＲＯＭ２０２或いはＨＤ２１１に記憶されたソフトウェア、或いはＦＤ２１２より供給されるソフトウェアを実行することで、システムバス２０４に接続された各構成部を総括的に制御する。すなわち、ＣＰＵ２０１は、所定の処理シーケンスに従った処理プログラムを、ＲＯＭ２０２、或いはＨＤ２１１、或いはＦＤ２１２から読み出して実行することで、後述する本実施の形態での動作を実現するための制御を行う。

【００３９】ＲＡＭ２０３は、ＣＰＵ２０１の主メモリ或いはワークエリア等として機能する。ＫＢＣ２０５は、ＫＢ２０９や図示していないポインティングデバイス等からの指示入力を制御する。ＣＲＴＣ２０６は、ＣＲＴ２１０の表示を制御する。ＤＫＣ２０７は、ブートプログラム、種々のアプリケーション、編集ファイル、ユーザファイル、ネットワーク管理プログラム、及び本実施の形態を実現するための所定の処理プログラム等を記憶するＨＤ２１１及びＦＤ２１２とのアクセスを制御する。ＮＩＣ２０８は、ネットワーク１４０上の装置或いはシステムと双方向にデータをやりとりする。

【００４０】ユーザ側の端末装置１１０（ｎ）は、上記図２のコンピュータ機能２００を有するパーソナルコンピュータ等を含み、ユーザからの操作に従って、ネットワーク１４０を介してサーバ１２０へアクセス等する。

【００４１】サーバ１２０は、詳細は後述するが、ユーザ側の端末装置１１０（ｎ）からのアクセスに基づいて、任意のサービスを提供する機能を有し、本実施の形態の最も特徴とする構成である。

【００４２】＜サーバ１２０の構成＞ネットワークシステム１００の特徴とする構成はサーバ１２０にあり、このサーバ１２０は、特に、提供するサービスに関する情報を記憶したデータベース１３０と連動して動作するサービス提供部１２１と、複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）と、複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）のユーザ認証結果に基づいて最終的なユーザ認証結果を判断する認証判断部１２３とを含み、これらの構成部１２１、１２２（１），１２２（２），・・・，１２２（ｎ）、及び１２３等により、ユーザ側の端末装置１１０（ｎ）からのサービス要求を受け付け、当該要求に含まれるユーザ認証に必要な情報を用いたユーザ認証の結果に従って、当該要求により示されるサービスを、ユーザ側の端末装置１１０（ｎ）に提供する。

【００４３】複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）は、入力パスワードによりユーザ認証を行うユーザ認証部１２２（１）（パスワード認証部）や、ＩＣカードに記憶された情報によりユーザ認証を行うユーザ認証部１２２（２）（ＩＣカード認証部）等を含んでいる。これらの複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）に対して、単一の認証判断部１２３が設けられている。

【００４４】例えば、ユーザ認証部１２２（１）は、ユーザ側の端末装置１１０（ｎ）からの、パスワード入力によるサービス要求（サービスを受けるためのユーザ認証の要求を含む）受け付ける。認証判断部１２３は、上記の入力パスワードと、サービスデータベース１３０内に予め秘密に保管している、該当サービスを受ける権利のあるユーザのパスワードとを比較し、これらのパスワードが一致した場合に、正しくユーザ認証されたと判断する。

【００４５】また、ユーザ認証部１２２（２）は、ユーザ側の端末装置１１０（ｎ）からの、ＩＣカード入力によるサービス要求（サービスを受けるためのユーザ認証の要求を含む）受け付ける。認証判断部１２３は、上記の

ＩＣカード上の情報と、サービスデータベース１３０内に予め秘密に保管している、該当サービスを受ける権利のあるユーザのＩＣカード上の情報とを比較し、これらのカード情報が一致した場合に、正しくユーザ認証されたと判断する。

【００４６】尚、複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）としては、上述したパスワードによりユーザ認証するユーザ認証部１２２（１）や、ＩＣカードによりユーザ認証するユーザ認証部１２２（２）に限られることはなく、指紋や声紋、或いは網膜パターン等の生体情報を利用したユーザ認証方法等のような、任意のユーザ認証方法でユーザ認証を行うユーザ認証部を含めるようにしてもよい。

【００４７】認証判断部１２３は、詳細は後述するが、上述のような複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）による複数のユーザ認証結果に基づいて、最終的なユーザ認証判断結果を決定する。

【００４８】サービス提供部１２１は、認証判断部１２３の最終的なユーザ認証結果に基づいて、サービス要求のあったユーザ側の端末装置１１０（ｎ）に対して該当するサービスを提供する。

【００４９】尚、サービス提供部１２１が提供するサービスについて、その数及び種類は限られるものではなく、単一或いは複数のサービスを提供可能である。

【００５０】また、ここでの「サービス」とは、「ユーザに対して、あるコンテンツを動作させる」と定義する。例えば、“コンテンツ”が“画像コンテンツ”であって、“動作”が“表示する”と決定した後に、“画像コンテンツを表示する”というサービスの提供が可能となる。

【００５１】また、本実施の形態におけるサービスとしては、様々なサービスを適用可能である。例えば、音声、或いは画像、或いは音楽及び画像等のコンテンツをユーザ側の端末装置１１０（ｎ）へ提供するサービスや、当該コンテンツをユーザ側の端末装置１１０（ｎ）で再生するサービス、或いは当該コンテンツ（画像のコンテンツ等）をユーザ側の端末装置１１０（ｎ）で表示或いは印刷出力するサービス等、様々なサービスを適用可能である。

【００５２】また、上記のサービスについて、例えば、ユーザ側の端末装置１１０（ｎ）へ提供するコンテンツの品質を変化させるようにしてもよい。例えば、ユーザ側の端末装置１１０（ｎ）で再生可能な音声のコンテンツの音質を変化させる。或いは、ユーザ側の端末装置１１０（ｎ）で印刷出力可能な画像のンテンツの画質を変化させる。これにより、ユーザ側の端末装置１１０（ｎ）に提供するサービスにレベルを持たせることが可能となる。

【００５３】また、ユーザ側の端末装置１１０（ｎ）に提供するサービスに関する情報は、上述したように、サービスデータベース１３０で保管されているが、これは、サービスデータベース１３０が、コンテンツと動作の双方を保管していることを意味する。

【００５４】＜サーバ１２０の認証判断部１２３の構成＞認証判断部１２３は、複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）による複数のユーザ認証結果に基づいて、最終的なユーザ認証判断結果を決定する手段である。ここでは説明の簡単のため、ユーザ認証部１２２（１）は、パスワードを用いたユーザ認証を行い、ユーザ認証部１２２（２）は、ＩＣカードを用いたユーザ認証を行い、ユーザ認証部１２２（３）は、指紋画像を用いたユーザ認証を行うものとし、これらの３つのユーザ認証部１２２（１）～１２２（３）による３つのユーザ認証結果に基づいて、認証判断部１２３は、最終的なユーザ認証判断結果を決定するものとする。

【００５５】図３は、上記の場合の、認証判断部１２３におけるユーザ認証判断結果の決定状態の遷移を示したものである。上記図３において、〔0〕～〔7〕で示す各頂点（黒丸点）は、ユーザ認証判断結果の決定後の状態を表し、各頂点を結ぶ各枝は、ユーザ認証された場合の動作を表す。

【００５６】すなわち、頂点〔0〕（“なし”）は、全てのユーザ認証に失敗している状態を表す。頂点〔1〕（“パスワード”）は、パスワードのみユーザ認証されている状態を表す。頂点〔2〕（“ＩＣカード”）は、ＩＣカードのみユーザ認証されている状態を表す。頂点〔3〕（“指紋（指紋画像）”）は、指紋のみユーザ認証されている状態を表す。頂点〔4〕（“パスワード＆ＩＣカード”）は、パスワード及びＩＣカードがユーザ認証されている状態を表す。頂点〔5〕（“パスワード＆指紋”）は、パスワード及び指紋がユーザ認証されている状態を表す。頂点〔6〕（“ＩＣカード＆指紋”）は、ＩＣカード及び指紋がユーザ認証されている状態を表す。頂点〔7〕（“パスワード＆ＩＣカード＆指紋”）は、パスワード、ＩＣカード、及び指紋の全てがユーザ認証されている状態を表す。

【００５７】認証判断部１２３は、上記図３で示される遷移状態に従って、３つのユーザ認証部１２２（１）～１２２（３）による３つのユーザ認証結果（パスワード、ＩＣカード、及び指紋によるユーザ認証結果）に基づいて、最終的なユーザ認証判断結果を段階的に決定する。

【００５８】例えば、認証判断部１２３は、先ず、頂点〔0〕（“なし”）の状態を初期状態とする。この初期状態において、パスワードによるユーザ認証に成功した場合（ユーザ認証部１２２（１）のユーザ認証結果がＯＫの場合）、認証判断部１２３は、頂点〔1〕（“パスワード”）の状態へ移行する。 次に、この状態において、

ＩＣカードによるユーザ認証に成功した場合（ユーザ認証部１２２（２）のユーザ認証結果がＯＫの場合）、認証判断部１２３は、頂点〔4〕（“パスワード＆ＩＣカード”）の状態へ移行する。

【００５９】上述のように、認証判断部１２３は、複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）による複数のユーザ認証結果に基づいて、ユーザ認証状態を遷移させることで、最終的なユーザ認証判断結果を段階的に決定する。

【００６０】＜サーバ１２０のサービスデータベース１３０の構成＞サービスデータベース１３０は、コンテンツ及びコンテンツに対する動作を含むサービスを保管するためのものであると共に、ユーザ認証判断結果、及びサービスに対応したアクセス制御リストを保管するためのものである。サーバ１２０は、サービスデータベース１３０内の保管情報（ユーザ認証判断結果情報及びアクセス制御リスト等）に基づいて、サービス提供部１２１により、サービス提供を制御する。

【００６１】サービスデータベース１３０で管理するアクセス制御リストについては、例えば、パスワードを用いたユーザ認証、ＩＣカードを用いたユーザ認証、及び指紋を用いたユーザ認証の３つのユーザ認証結果に基づいて、最終的なユーザ認証判断結果を決定する場合、当該アクセス制御リストは、３次元的な構成をなすリストとなる。

【００６２】図４は、上記の場合において、コンテンツが画像コンテンツである場合のアクセス制御リストの一例を示したものである。上記図４において、縦軸の“頂点〔0〕～〔7〕”は、認証判断部１２３の最終的なユーザ認証判断結果を示す。

【００６３】具体的には例えば、ここでは、パスワードを用いたユーザ認証、ＩＣカードを用いたユーザ認証、及び指紋を用いたユーザ認証の３つのユーザ認証結果から最終的なユーザ認証結果を決定するため、上記図３に示したユーザ認証状態遷移が想定される。したがって、上記図４では、当該ユーザ認証状態遷移を縦軸としている。また、上記図４において、横軸は、画像コンテンツに対する多様化したサービスの示す。ここでは、「低解像度表示」、「高解像度表示」、「低解像度編集」、及び「高解像度編集」の４段階のサービスとしている。そして、縦軸（ユーザ認証状態）と、横軸（サービス）との交点の“○”（サービス許可）或いは“×”（サービス不許可）は、当該サービスを許可するか否か（画像コンテンツの表示或いは編集の動作）を示している。

【００６４】尚、ここでは、画像コンテンツの表示及び編集のサービスを提供するものとし、アクセス制御リストを、上記図４に示したようなリストとしているが、これに限られることはない。例えば、画像コンテンツの印刷のサービスを提供するようにしてもよい。また、サービスの段階についても上記図４に示したものに限られることはなく、例えば、「中解像度のコンテンツを印刷する」等のような、他の様々な形態のサービスを存在させるようにしてもよい。

【００６５】また、上記図４に示したように、本実施の形態では、ユーザ認証判断結果、すなわち、上記図３に示したユーザ認証状態遷移における頂点〔x〕の位置によって、サービスの許可／不許可（アクセス制御）を決定することを特徴としているが、上記図４に示したようなアクセス制御リストに関しては特に制限しない。

【００６６】例えば、図５に示すようなアクセス制御リストにより、アクセス制御を決定するようにしてもよい。この場合、 全てのユーザ認証でユーザ認証結果がＯＫでない限り、サービスが許可されない。これにより、最も強固なユーザ認証を実現するができる。

【００６７】また、例えば、図６に示すようなアクセス制御リストにより、アクセス制御を決定するようにしてもよい。この場合、何れか1つのユーザ認証でユーザ認証結果がＯＫである場合、画像コンテンツの表示に関するサービスが全て許可される。また、何れか２つのユーザ認証でユーザ認証結果がＯＫである場合、画像コンテンツの編集に関するサービスをも全て許可される。すなわち、この場合、全てのユーザ認証でのユーザ認証結果がＯＫでなくても、1つ或いは２つのユーザ認証でのユーザ認証結果がＯＫであれば、該当する段階（レベル）のサービスを受けることが可能となる。これにより、例えば、ユーザ認証に必要なＩＣカードの紛失や盗難等の認証情報の保管に関する信頼性を向上させることができる。

【００６８】また、例えば、図７に示すようなアクセス制御リストにより、アクセス制御を決定するようにしてもよい。この場合、ＩＣカードの利用を前提とするシステム設計の要求に応じることができる。具体的には例えば、セキュリティを考慮したシステムにおいては、ＩＣカードを利用したシステムが実用化されている。このことから、ＩＣカードの利用を前提とするシステム設計が要求されることが考えられる。したがって、上記図７のアクセス制御リストを生成することで、上記の要求を実現できる。

【００６９】上記図７のアクセス制御リストでは、ＩＣカードを用いたユーザ認証結果がＯＫである場合、すなわち頂点〔2〕、頂点〔4〕、頂点〔6〕、及び頂点〔7〕（上記図３参照）の各ユーザ認証状態においては、サービスが全てを許可されるが、他の頂点のユーザ認証状態では、全てのサービスが許可されない。

【００７０】また、上記図７のアクセス制御リストと共に、上記図６のアクセス制御リストを用いて、アクセス制御を決定するようにしてもよい。この場合、例えば、ユーザは、ＩＣカードがない場合であっても、単一又は複数のＩＣカード以外の、ユーザ認証を行うための手段（パスワードや指紋等）を用いて、ＩＣカードによるユ

ーザ認証の結果により許可されるサービスと同等のサービスを受けることができる。

【００７１】＜ネットワークシステム１００の動作＞図８は、ネットワークシステム１００の動作を示したものである。例えば、ユーザ側の端末装置１１０（ｎ）及びサーバ１２０が備えるコンピュータ機能２００において、ＣＰＵ２０１は、上記図８のフローチャートに従った処理プログラムを実行する。これにより、ネットワークシステム１００は、次のように動作する。

【００７２】ステップＳ３０１：ユーザは、自端末装置１１０（ｎ）により、サーバ１２０に対してサービス要求（ユーザ認証要求）を発行する。

【００７３】ステップＳ３０２：サーバ１２０において、複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）の中の該当するユーザ認証部（以下、「ユーザ認証部１２２（ｘ）」とする）は、ユーザ側の端末装置１１０（ｎ）からの要求を受け付ける。例えば、ユーザがパスワード入力により当該要求を発行した場合には、パスワードによるユーザ認証を行うユーザ認証部１２２（１）が当該要求を受け付ける。認証判断部１２３は、ユーザ認証部１２２（ｘ）で受け付けられた要求に基づいたユーザ認証結果に従って、上記図３に示したようなユーザ認証状態を遷移させる。

【００７４】ステップＳ３０３：ユーザは、自端末装置１１０（ｎ）により、他のユーザ認証方法によりサーバ１２０に対してサービス要求（ユーザ認証要求）する場合、当該サービス要求をサーバ１２０に対して発行する。この場合、再びステップＳ３０１からの処理が繰り返し実行される。一方、ユーザが、他のユーザ認証方法によりサーバ１２０に対してサービス要求（ユーザ認証要求）しない場合、次のステップＳ３０４からの処理に進む。

【００７５】ステップＳ３０４：サーバ１２０において、認証判断部１２３は、ステップＳ３０１及びＳ３０２の結果（単一又は複数のユーザ認証結果に基づいた最終的なユーザ認証状態の遷移結果）を定める。

【００７６】ステップＳ３０５：サービス提供部１２１は、認証判断部１２３で得られた最終的なユーザ認証判断結果、及び上記図４等に示したアクセス制御リストに基づいて、アクセス制御を決定し、該当するサービスを、ユーザ側の端末装置１１０（ｎ）に対して許可、又は不許可する。

【００７７】上述のように、本実施の形態では、複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）によりユーザ認証を行い、それぞれのユーザ認証結果から、段階的なユーザ認証判断結果を最終的に決定し、そのユーザ認証判断結果に基づいて、段階的なサービスを提供するように構成した。すなわち、従来では、サービスに固定のユーザ認証方法のみが提供され、ユーザの認証結果に対して提供されるサービスが一意に決まっていた構成に対して、本実施の形態では、段階的なユーザ認証判断結果を取得し、それに応じて適応的なサービスを提供することを実現した。これにより、ユーザのサービス享受の環境に適応的に対応してサービスを提供することができる。

【００７８】〔第２の実施の形態〕本発明は、例えば、図９に示すようなネットワークシステム４００（Ａ）に適用される。本実施の形態のネットワークシステム４００（Ａ）は、特に、上記図９に示すように、上記図１に示したネットワークシステム１００の構成に対して、２つのサーバ１２０（１），１２０（２）を設けた構成が異なる。

【００７９】尚、上記図９のネットワークシステム４００（Ａ）において、上記図１のネットワークシステム１００と同様に動作する箇所には同じ符号を付し、その詳細な説明は省略する。

【００８０】すなわち、本実施の形態では、ユーザ認証を行うサーバ（認証サーバ）１２０（１）と、サービスを提供するサーバ（サービス提供サーバ）１２０（２）とを分けて設けるようにする。

【００８１】サーバ１２０（１）は、複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）及び認証判断部１２３を含み、サーバ１２０（２）は、サービス提供部１２１及びサービスデータベース１３０を含んでいる。そして、これらのサーバ１２０（１），１２０（２）は、上記図１のサーバ１２０と同様に、ネットワーク１４０上に接続されている。

【００８２】したがって、ユーザは、自端末装置１１０（ｎ）により、サーバ１２０（１）に対して、サーバ１２０（２）からサービスを受けるためのユーザ認証要求を発行する。

【００８３】サーバ１２０（１）は、ユーザ側の端末装置１１０（ｎ）からの要求に基づいて、ユーザ認証を行い、その結果（最終的なユーザ認証判断結果）をサーバ１２０（２）へ送信する。サーバ１２０（２）は、サーバ１２０（１）からのユーザ認証判断結果に基づいて、ユーザ側の端末装置１１０（ｎ）のアクセス制御を決定する。

【００８４】〔第３の実施の形態〕本発明は、例えば、図１０に示すようなネットワークシステム４００（Ｂ）に適用される。本実施の形態のネットワークシステム４００（Ｂ）は、特に、上記図１０に示すように、上記図１に示したネットワークシステム１００の構成に対して、２つのサーバ１２０（３），１２０（４）を設けた構成が異なる。

【００８５】尚、上記図１０のネットワークシステム４００（Ｂ）において、上記図１のネットワークシステム１００と同様に動作する箇所には同じ符号を付し、その詳細な説明は省略する。

【００８６】すなわち、本実施の形態では、ユーザ認証

を行う2つのサーバ（認証サーバ）１２０（３）及び１２０（４）を分けて設けるようにする。

【００８７】サーバ１２０（３）は、複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）の中の単一又は複数のユーザ認証部（上記図１０では、ユーザ認証部１２２（ｘ）以外のユーザ認証部）、認証判断部１２３、サービス提供部１２１、及びサービスデータベース１３０を含んでいる。サーバ１２０（４）は、複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）の中の単一又は複数のユーザ認証部（上記図１０では、ユーザ認証部１２２（ｘ））を含んでいる。そして、これらのサーバ１２０（３），１２０（４）は、上記図１のサーバ１２０と同様に、ネットワーク１４０上に接続されている。

【００８８】したがって、ユーザは、自端末装置１１０（ｎ）により、サーバ１２０（３）或いはサーバ１２０（４）に対して、サーバ１２０（３）からサービスを受けるためのユーザ認証要求を発行する。

【００８９】サーバ１２０（３）は、ユーザ側の端末装置１１０（ｎ）からの要求に基づいて、外部のサーバ１２０（４）のユーザ認証部、或いは内部のユーザ認証部によりユーザ認証を行い、その結果（最終的なユーザ認証判断結果）に基づいて、ユーザ側の端末装置１１０（ｎ）のアクセス制御を決定する。

【００９０】尚、上記図9のネットワークシステム４００（Ａ）の構成、及び上記図１０のネットワークシステム４００（Ｂ）の構成を組み合わせて新たなネットワークシステムを構成しするようにしてもよい。すなわち、ユーザ認証を行うサーバと、サービスを提供するサーバとを、それぞれ複数備えるネットワークシステムを構成してもよい。

【００９１】〔第４の実施の形態〕本発明は、例えば、図１１に示すようなネットワークシステム５００に適用される。本実施の形態のネットワークシステム５００は、上記図１１に示すように、上記図１のネットワークシステム１００に対して、サーバ１２０が接続しているネットワーク１４０（１）と、これに対して外部のネットワーク（外部ネットワーク）１４０（２）とを備えている。

【００９２】このため、ネットワークシステム５００のユーザ側の端末装置としては、ネットワーク（内部ネットワーク）１４０（１）を介してサーバ１２０へアクセスするユーザ側の端末装置１１０（１）、及び外部ネットワーク１４０（２）を介してサーバ１２０へアクセスするユーザ側の端末装置１１０（２）が存在する。

【００９３】また、サーバ１２０は、上記図１に示した構成に加えて、さらに詳細は後述する位置検出部１２４を備える構成としている。

【００９４】尚、上記図１１のネットワークシステム５００において、上記図１のネットワークシステム１００と同様に動作する箇所には同じ符号を付し、その詳細な説明は省略する。

【００９５】サーバ１２０において、位置検出部１２４は、サービス要求（ユーザ認証要求）を発行したユーザ側の端末装置の位置を検出（内部ネットワーク１４０（１）上に位置するか、外部ネットワーク１４０（２）上に位置するかを検出）する。

【００９６】尚、上記の“ネットワーク上の位置”は、例えば、ユーザ側の端末装置のＩＰアドレス、或いはユーザ側の端末装置が存在するネットワーク名、或いはユーザ側の端末装置のネットワーク上での論理的な位置等を含む。また、位置検出部１２４での位置検出方法としては、例えば、ユーザ側の端末装置から別途送出された位置情報により位置を検出する方法、或いはＩＰケットから位置を検出する方法等のように、ユーザ側の端末装置から送られてきた情報により、自動的に当該端末装置の位置を検出する方法等が適用可能あるが、特に限定しない。

【００９７】認証判断部１２３は、第１の実施の形態と同様に、複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）によりユーザ認証を行い、それぞれのユーザ認証結果から、段階的なユーザ認証判断結果を最終的に決定するが、この決定の際に、位置検出部１２４での検出結果をも含めて、当該決定を行う。

【００９８】例えば、位置検出部１２４において、ユーザ認証要求を発行したユーザ側の端末装置が、サーバ１２０と同じネットワーク１４０（１）上に存在する、と検出された場合、認証判断部１２３は、基準を低くして（アクセス制御リストでのサービス許可の基準を低くして）、上記のユーザ認証判断結果を決定する。また、位置検出部１２４において、ユーザ認証要求を発行したユーザ側の端末装置が、サーバ１２０と異なるネットワーク１４０（２）上に存在する、と検出された場合、認証判断部１２３は、基準を高くして（アクセス制御リストでのサービス許可の基準を高くして）、上記のユーザ認証判断結果を決定する。

【００９９】具体的には例えば、まず、図１２は、上記図１１のネットワークシステム５００を、社内システム５００´に適用した場合の構成を示したものである。この場合、サーバ１２０が「社内サーバ」として機能し、ネットワーク（内部ネットワーク）１４０（１）が社内ネットワークとして機能し、ネットワーク（外部ネットワーク）１４０（２）が社外ネットワークとして機能する。また、社内ネットワーク１４０（１）上のユーザ側の端末装置１１０（１）が、社内の社員が使用する端末装置に相当し、社外ネットワーク１４０（２）上のユーザ側の端末装置１１０（２）が、社外の者が使用する端末装置に相当する。

【０１００】図１３及び図１４は、上記図１２の社内シ

ステム５００´において、パスワードを用いたユーザ認証、ＩＣカードを用いたユーザ認証、及び指紋を用いたユーザ認証の３つのユーザ認証結果から最終的なユーザ認証結果を決定するものとし、且つコンテンツを画像コンテンツとした場合の、アクセス制御リストの一例を示したものである。

【０１０１】上記図１３のアクセス制御リストは、社内ネットワーク１４０（１）上に接続されたユーザ側の端末装置１１０（１）からのユーザ認証要求に対するアクセス制御リストであり、このアクセス制御リストにおいては、ユーザ側の端末装置１１０（１）に対して、1つ以上のユーザ認証でのユーザ認証結果がＯＫであれば、該当するサービスが許可される。

【０１０２】上記図１４のアクセス制御リストは、社外ネットワーク１４０（２）上に接続されたユーザ側の端末装置１１０（２）からのユーザ認証要求に対するアクセス制御リストであり、このアクセス制御リストにおいては、ユーザ側の端末装置１１０（２）に対して、３つの全てのユーザ認証でのユーザ認証結果がＯＫでないと、該当するサービスが許可されない。

【０１０３】したがって、認証判断部１２３は、位置検出部１２４の検出結果が、ユーザ認証要求を発行したユーザ側の端末装置がサーバ１２０と同じネットワーク１４０（１）上に存在するという結果である場合、上記図１３のアクセス制御リストにより、サービス提供許可の基準を低くして、最終的なユーザ認証判断結果を決定する。また、認証判断部１２３は、位置検出部１２４の検出結果が、ユーザ認証要求を発行したユーザ側の端末装置がサーバ１２０と異なるネットワーク１４０（２）上に存在するという結果である場合、上記図１４のアクセス制御リストにより、サービス提供許可の基準を高くして、最終的なユーザ認証判断結果を決定する。

【０１０４】上述のように、本実施の形態では、認証判断部１２３にて最終的なユーザ認証判断結果を決定する際に、複数のユーザ認証部１２２（１），１２２（２），・・・，１２２（ｎ）による複数のユーザ認証結果だけでなく、ユーザ認証の対象となっているユーザ側の端末装置の位置情報を加味して、当該決定を行うように構成したので、より柔軟にユーザ認証のレベルを決定することができる。

【０１０５】尚、本発明の目的は、第１～第４の実施の形態のホスト及び端末の機能を実現するソフトウェアのプログラムコードを記憶した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（又はＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読みだして実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が第１～第４の実施の形態の機能を実現することとなり、そのプログラムコードを記憶した記憶媒体は本発明を構成することとなる。プログラムコードを供給するための記憶媒体としては、ＲＯＭ、フロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード等を用いることができる。また、コンピュータが読みだしたプログラムコードを実行することにより、第１～第４の実施の形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳ等が実際の処理の一部又は全部を行い、その処理によって第１～第４の実施の形態の機能が実現される場合も含まれることは言うまでもない。さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された拡張機能ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部又は全部を行い、その処理によって第１～第４の実施の形態の機能が実現される場合も含まれることは言うまでもない。

【０１０６】

【発明の効果】以上説明したように本発明では、ユーザからの要求（パスワードやＩＣカード等による任意のサービス提供要求等）に基づいて、当該ユーザの認証を行う際に、単一又は複数のユーザ認証方法（パスワードを用いたユーザ認証方法、ＩＣカードを用いたユーザ認証方法、バイオメトリクスを用いたユーザ認証方法等）による単一又は複数のユーザ認証結果に基いて、最終的なユーザ認証結果を段階的に決定するように構成した。具体的には例えば、従来のように１つのユーザ認証方法に依存した１種類の情報から得られる「可」又は「不可」の二値のユーザ認証結果ではなく、複数のユーザ認証方法による複数のユーザ認証結果の組み合わせに基いて、多値のユーザ認証結果を出力できるように構成した。これにより、段階的なユーザ認証結果に基いて、サービスの質を段階的に変える等して、ユーザにサービスを提供することができる。

【０１０７】また、上記の最終的なユーザ認証結果を段階的に決定する際に、ユーザからの要求がなされた装置或いはシステム等の存在位置をも加味するように構成した場合、より柔軟にユーザ認証結果の段階を決定することができる。

【０１０８】したがって、本発明によれば、

（１）多様なサービス提供形態に対応できる。

（２）段階的であって多様なサービスを提供する際に、それぞれのサービスに対応可能である。

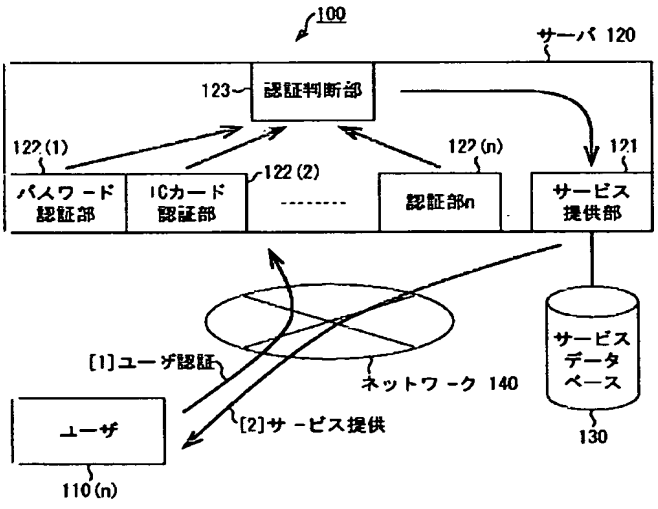
（３）ユーザ認証結果に応じて適応的に異なるサービスを提供できる。という効果を得ることができる。

【図面の簡単な説明】

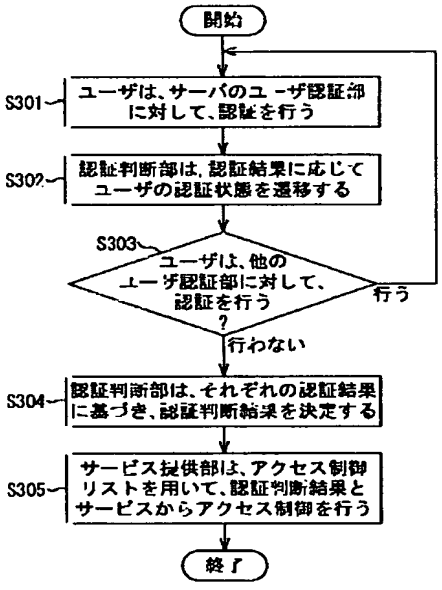
【図１】第１の実施の形態において、本発明を適用したネットワークシステムの構成を示すブロック図である。

【図２】上記ネットワークシステム内のサーバ及びユーザ側の端末装置が有するコンピュータ機能の構成を示すブロック図である。
【図３】上記サーバにおいて、認証判断部が最終的なユーザ認証判断結果を決定する際の、ユーザ認証状態の遷移を説明するための図である。
【図４】上記サーバにおいて、サービス提供部が上記ユーザ認証判断結果に基づいて段階的なサービス許可／不許可を決定するためのアクセス制御リストを説明するための図である。
【図５】上記アクセス制御リストの他の例（例１）を説明するための図である。
【図６】上記アクセス制御リストの他の例（例２）を説明するための図である。
【図７】上記アクセス制御リストの他の例（例３）を説明するための図である。
【図８】上記ネットワークシステムの動作を説明するためのフローチャートである。
【図９】第２の実施の形態において、本発明を適用したネットワークシステムの構成を示すブロック図である。
【図１０】第３の実施の形態において、本発明を適用したネットワークシステムの構成を示すブロック図である。
【図１１】第４の実施の形態において、本発明を適用したネットワークシステムの構成を示すブロック図である。
【図１２】上記ネットワークシステムを社内システムに適用した場合の構成を示すブロック図である。
【図１３】上記社内システムのサーバにおいて、サービス提供部がユーザ認証判断結果に基づいて段階的なサービス許可／不許可を決定するためのアクセス制御リスト（社内からのユーザ認証要求の場合のリスト）を説明するための図である。
【図１４】上記社内システムのサーバにおいて、サービス提供部がユーザ認証判断結果に基づいて段階的なサービス許可／不許可を決定するためのアクセス制御リスト（社外からのユーザ認証要求の場合のリスト）を説明するための図である。
【符号の説明】
１００　ネットワークシステム
１１０（ｎ）　ユーザ側の端末装置
１２０　サーバ
１２１　サービス提供部
１２２（１），１２２（２），・・・，１２２（ｎ）　ユーザ認証部
１２３　認証判断部
１３０　サービスデータベース
１４０　ネットワーク

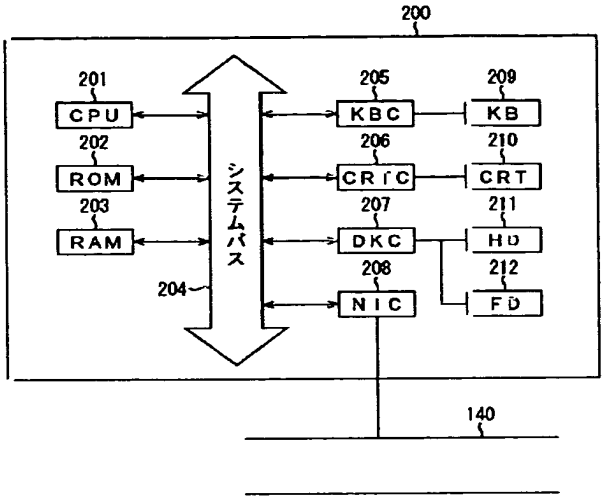
【図１】



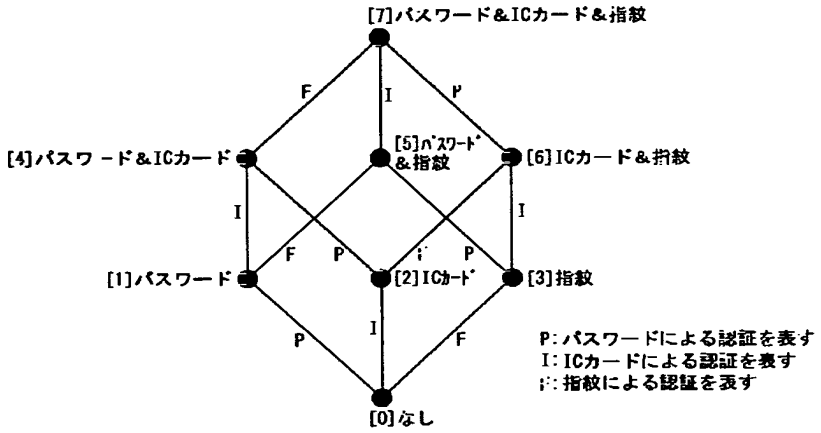
【図８】



【図2】


200
201
CPU
202
ROM
203
RAM
204
システムバス
205
KBC
206
CRTC
207
DKC
208
NIC
209
KB
210
CRT
211
HD
212
FD
140

【図3】


[7]パスワード&ICカード&指紋
F
I
P
[4]パスワード&ICカード
[5]パスワード&指紋
[6]ICカード&指紋
I
I
F
P
P
[1]パスワード
[2]ICカード
[3]指紋
P
I
F
[0]なし
P:パスワードによる認証を表す
I:ICカードによる認証を表す
F:指紋による認証を表す

【図４】

○：サービスを許可
×：サービスを不許可

	低解像度表示	高解像度表示	低解像度編集	高解像度編集
頂点0	×	×	×	×
頂点1	○	×	×	×
頂点2	○	×	×	×
頂点3	○	×	×	×
頂点4	○	○	×	×
頂点5	○	○	○	×
頂点6	○	○	○	×
頂点7	○	○	○	○

【図５】

○：サービスを許可
×：サービスを不許可

	低解像度表示	高解像度表示	低解像度編集	高解像度編集
頂点0	×	×	×	×
頂点1	×	×	×	×
頂点2	×	×	×	×
頂点3	×	×	×	×
頂点4	×	×	×	×
頂点5	×	×	×	×
頂点6	×	×	×	×
頂点7	○	○	○	○

【図６】

○：サービスを許可
×：サービスを不許可

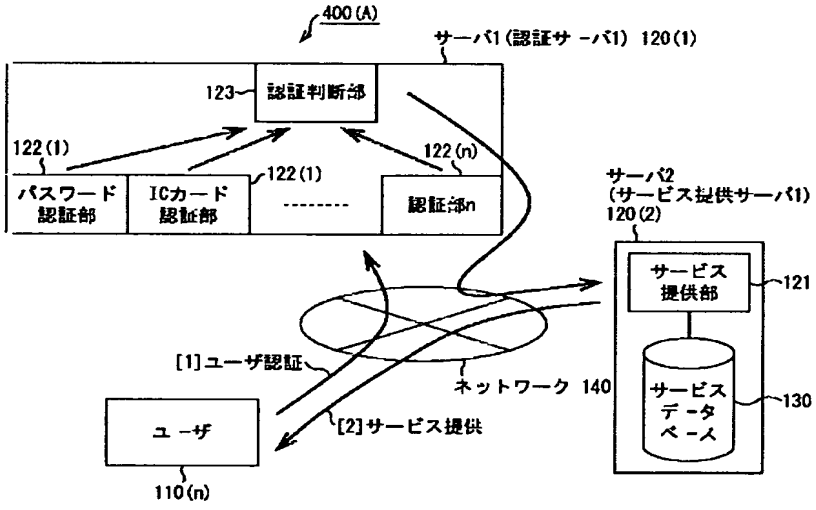
	低解像度表示	高解像度表示	低解像度編集	高解像度編集
頂点0	×	×	×	×
頂点1	○	○	×	×
頂点2	○	○	×	×
頂点3	○	○	×	×
頂点4	○	○	○	○
頂点5	○	○	○	○
頂点6	○	○	○	○
頂点7	○	○	○	○

【図7】

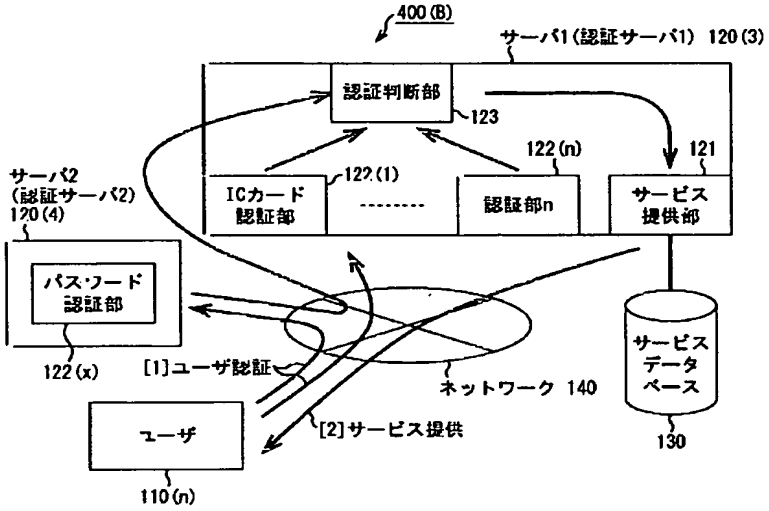
○：サービスを許可
×：サービスを不許可

	低解像度表示	高解像度表示	低解像度編集	高解像度編集
頂点0	×	×	×	×
頂点1	×	×	×	×
頂点2	○	○	○	○
頂点3	×	×	×	×
頂点4	○	○	○	○
頂点5	×	×	×	×
頂点6	○	○	○	○
頂点7	○	○	○	○

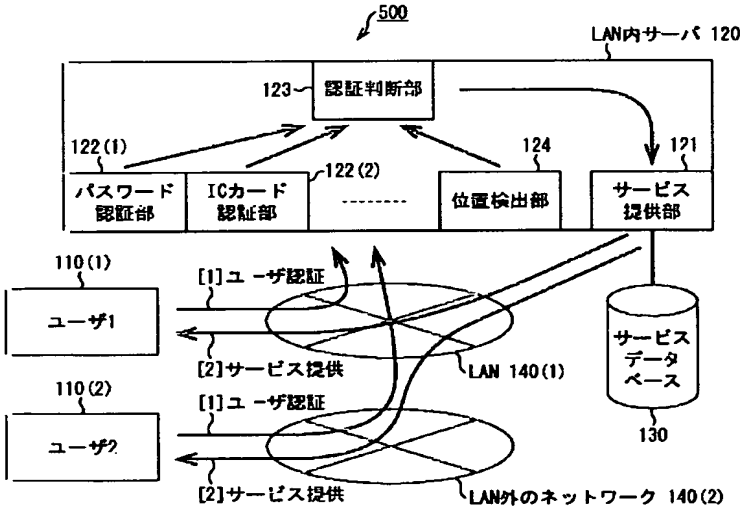
【図9】



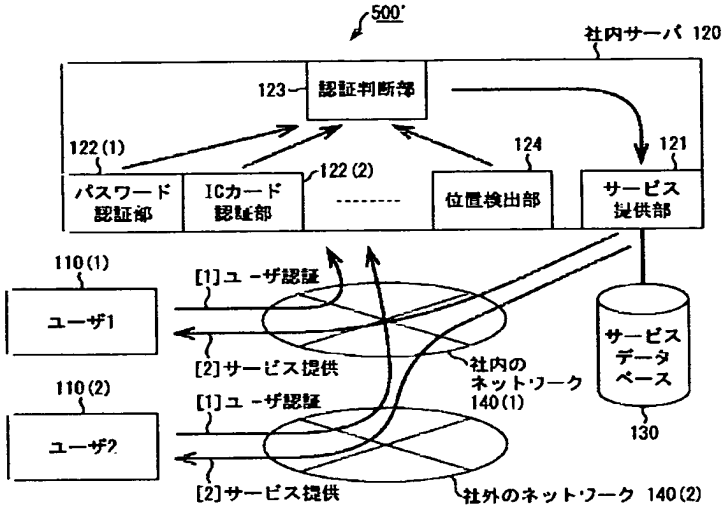
【図１０】


400(B)
サーバ1(認証サーバ1) 120(3)
認証判断部
123
122(n)
121
ICカード認証部
122(1)
認証部n
サービス提供部
サーバ2
(認証サーバ2)
120(4)
パスワード認証部
122(x)
[1]ユーザ認証
ネットワーク 140
サービスデータベース
130
ユーザ
[2]サービス提供
110(n)

【図１１】


500
LAN内サーバ 120
123
認証判断部
122(1)
124
121
パスワード認証部
ICカード認証部
122(2)
位置検出部
サービス提供部
110(1)
[1]ユーザ認証
ユーザ1
[2]サービス提供
LAN 140(1)
サービスデータベース
130
110(2)
[1]ユーザ認証
ユーザ2
[2]サービス提供
LAN外のネットワーク 140(2)

【図１２】



【図１３】

○：サービスを許可
×：サービスを不許可

	低解像度表示	高解像度表示	低解像度編集	高解像度編集
社内ユーザ頂点0	×	×	×	×
社内ユーザ頂点1	○	○	○	○
社内ユーザ頂点2	○	○	○	○
社内ユーザ頂点3	○	○	○	○
社内ユーザ頂点4	○	○	○	○
社内ユーザ頂点5	○	○	○	○
社内ユーザ頂点6	○	○	○	○
社内ユーザ頂点7	○	○	○	○

【図１４】

○：サービスを許可
×：サービスを不許可

	低解像度表示	高解像度表示	低解像度編集	高解像度編集
社外ユーザ頂点0	×	×	×	×
社外ユーザ頂点1	×	×	×	×
社外ユーザ頂点2	×	×	×	×
社外ユーザ頂点3	×	×	×	×
社外ユーザ頂点4	×	×	×	×
社外ユーザ頂点5	×	×	×	×
社外ユーザ頂点6	×	×	×	×
社外ユーザ頂点7	○	○	○	○

フロントページの続き

(72)発明者　若尾　聡
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

Ｆターム(参考)　5B085 AE02 AE06 AE23
5J104 AA07 KA01 KA17 KA20 MA01
NA05 NA33 PA07